T. Ikeda 3300-01

1/24/01

Q62762

1 of 1

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２６日

出願番号
Application Number: 特願２０００－０２１８１０

出願人
Applicant(s): 新潟日本電気株式会社

２０００年１１月１７日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９６４６０

【書類名】　特許願

【整理番号】　03101929

【提出日】　平成12年 1月26日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

G06F 12/14

【発明者】

【住所又は居所】　新潟県柏崎市大字安田７５４６番地

新潟日本電気株式会社内

【氏名】　池田 剛

【特許出願人】

【識別番号】　000190541

【住所又は居所】　新潟県柏崎市大字安田７５４６番地

【氏名又は名称】　新潟日本電気株式会社

【代理人】

【識別番号】　100084250

【弁理士】

【氏名又は名称】　丸山 隆夫

【電話番号】　03-3590-8902

【手数料の表示】

【予納台帳番号】　007250

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書 1

【物件名】　図面 1

【物件名】　要約書 1

【包括委任状番号】　9800081

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報暗号化装置及びその方法

【特許請求の範囲】

【請求項１】　他の端末に対して重複することのない固有情報を格納する固有情報格納手段と、

前記固有情報を基にデータを暗号化する暗号化手段とを有することを特徴とする情報暗号化装置。

【請求項２】　前記固有情報を基に前記暗号化手段により暗号化されたデータを復号化する復号化手段をさらに有することを特徴とする請求項１記載の情報暗号化装置。

【請求項３】　前記固有情報格納手段は、格納した前記固有情報に対し、読み出すことのみ許可することを特徴とする請求項１または２記載の情報暗号化装置。

【請求項４】　前記暗号化手段により暗号化したデータを格納する記憶手段をさらに有することを特徴とする請求項１から３のいずれかに記載の情報暗号化装置。

【請求項５】　前記記憶手段は、実際にデータが書き込まれる記憶媒体が交換されないように構成されていることを特徴とする請求項１から４のいずれかに記載の情報暗号化装置。

【請求項６】　前記記憶手段は、前記実際にデータが書き込まれる記憶媒体が交換されるように構成されていることを特徴とする請求項１から４のいずれかに記載の情報暗号化装置。

【請求項７】　前記データを取り込むデータ取込手段をさらに有することを特徴とする請求項１から５のいずれかに記載の情報暗号化装置。

【請求項８】　前記固有情報格納手段は、ユーザに到達する以前に前記固有情報が格納されることを特徴とする請求項１から６のいずれかに記載の情報暗号化装置。

【請求項９】　前記固有情報格納手段は、レジスタにより構成されていることを特徴とする請求項１から８のいずれかに記載の情報暗号化装置。

【請求項１０】　前記固有情報は、各端末に割り当てられたシリアルナンバーであることを特徴とする請求項１から９のいずれかに記載の情報暗号化装置。

【請求項１１】　他の端末に対して重複することのない固有情報を基にデータを暗号化する暗号化工程を有することを特徴とする情報暗号化方法。

【請求項１２】　前記固有情報を基に前記暗号化工程において暗号化されたデータを復号化する復号化工程をさらに有することを特徴とする請求項１１記載の情報暗号化方法。

【請求項１３】　前記固有情報は、ユーザにより変更されないように保持されていることを特徴とする請求項１１または１２記載の情報暗号化方法。

【請求項１４】　前記暗号化工程において暗号化したデータを格納する記憶工程をさらに有することを特徴とする請求項１１から１３のいずれかに記載の情報暗号化方法。

【請求項１５】　前記記憶工程は、実際にデータが書き込まれる記憶媒体が交換されないように構成されている記憶媒体に前記暗号化したデータを書き込むことを特徴とする請求項１１から１４のいずれかに記載の情報暗号化方法。

【請求項１６】　前記記憶工程は、前記実際にデータが書き込まれる記憶媒体が交換されるように構成されている記憶媒体に前記暗号化したデータを書き込むことを特徴とする請求項１１から１４のいずれかに記載の情報暗号化方法。

【請求項１７】　前記暗号化工程の前に、前記データを取り込むデータ取込工程をさらに有することを特徴とする請求項１１から１５のいずれかに記載の情報暗号化方法。

【請求項１８】　前記固有情報は、レジスタに格納されていることを特徴とする請求項１１から１７のいずれかに記載の情報暗号化方法。

【請求項１９】　前記固有情報は、各端末に割り当てられたシリアルナンバーであることを特徴とする請求項１１から１８のいずれかに記載の情報暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パーソナルコンピュータ等の情報処理機器において外部情報を複製する情報暗号化装置及びその方法に関し、特にその複製された情報を使用できる機器をその複製処理を実行した情報処理機器に制限する情報暗号化装置及びその方法に関する。

【０００２】

【従来の技術】

近年、ハードディスクドライブ（ＨＤＤ）の記憶容量の大容量化や書き込み可能なＤＶＤ－ＲＡＭ（Digital Video Disk-Random Access Memor）やＣＤ－Ｒ（Compact Disk-Recordable）等の比較的大容量の記憶容量を有する記憶メディアの発達に伴い、映画等に代表される長時間の映像情報や音声情報をパーソナルコンピュータを介して記憶メディアに格納することが可能になってきている。

【０００３】

しかしながら、これら映像情報や音声情報には著作権が設定されているため、その利用範囲が、読み込み専用のＣＤやＤＶＤに限定されている。

【０００４】

このため、ＣＤやＤＶＤの再生機能を予め備えている比較的大型な情報処理機器での利用においては不便さを感じないが、近年普及している携帯性を重視した情報処理機器ではＣＤやＤＶＤの再生機能を内蔵しているものが少なく、拡張機能として外付けの再生機器によらなければならないため携帯性を損なうこととなってしまう。

【０００５】

この問題を解決する手段としては、対象となる映像情報や音声情報を情報処理機器に内蔵しているＨＤＤなどの記憶メディアに記憶させる方法が考えられるが、この方法においてデータをそのまま記憶メディアに格納できる場合、映像情報や音声情報の複製を容易にし、上記のような著作権の侵害を促進させてしまうという問題が生じる恐れがある。

【０００６】

加えて、上記のようにＨＤＤなどの記憶メディアを用いた複製は発見すること

が難しく、取り締まることが困難である。

【０００７】

そこで、著作権が設定されているデータをＨＤＤなどの記憶メディアに記憶できるように構成することにより発生するであろう著作権侵害の問題を防止するためには、対象となるデータを複製することで得られた産物を利用できる範囲を制限することが考えられる。

【０００８】

【発明が解決しようとする課題】

しかしながら、従来の技術による情報（データ）の暗号化では、ユーザの意志によりその暗号化する鍵データを決定しているため、ユーザのモラルに依存する形となっており、上記のような著作権の侵害をユーザに依存せずに防止する構成となっていない。

【０００９】

例えば、従来技術１として、特開昭６３－１３１７５７号公報によるボイスメール装置は、暗号化の対象となる音声情報をユーザに明らかな所定の暗号キーワードを用いて外部接続された暗号化復号化装置により暗号化し、同じく外部接続してある外部記憶装置に記憶するよう構成されている。このため、従来技術１では、上記のように暗号化したデータ（音声情報）を利用するために、ユーザに自明な暗号解読キーを入力手段より入力し、暗号化復号化装置においてこの暗号解読キーを用いて復号化するように構成されている。

【００１０】

また、従来技術２として、特開平９－３２１７４９号公報によるオンラインセキュリティ制御方式で適用されている暗号化手段は、ホストコンピュータとターミナル装置との通信において送受信するデータをユーザＩＤを基に暗号化するためのものである。このため、この暗号化に使用する鍵データは、当然本人により決定することができるものであり、如何なる端末からでもこのユーザＩＤを入力することで使用することが可能である。

【００１１】

また、従来技術３として、特開平１－２７０１９１号公報によるメモリカード

で適用されている暗号化手段は、記憶メディアとなるメモリＩＣの入出力段に設けられ、キーデータに従いメモリＩＣに書き込むデータの暗号化を行う。ここで、暗号化及び復号化に使用するキーデータとして如何なるデータを使用するかは開示されておらず、更に、その構成においても、データの複製における暗号化を目的とはしていない。

【００１２】

上記のように暗号化キーをユーザが決定することが可能な暗号化方法に対して、暗号化キーを所定の乱数発生方法により決定するように構成された従来技術が以下の公開特許公報により開示されている。

【００１３】

例えば、従来技術４として、特開平１１－１９１０７９号公報による半導体集積回路では、Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ（ＲＯＭ）を製造するにあたり、すでに暗号化されたデータを基に作製したフォトマスクによりＲＯＭにデータを書き込む。これに対し、書き込んだデータの復号化では、暗号解読手段をデータの出力段に設け、この暗号解読手段において、入力手段を介してユーザから入力された復号化鍵コード若しくは他の記憶メディアに保持た復号化鍵コードを使用してＲＯＭ内のデータを復号化する。このように、従来技術４は、暗号化したデータをによりＲＯＭに書き込みを行っているため、このＲＯＭ内に格納されたデータを複製すること自体を防止するためのものとなっている。

【００１４】

更に、従来技術５として、特開平１１－２３４２６１号公報による集積回路に適用される暗号化・復号化手段は、暗号化関数を特徴づけるパラメータを暗号化鍵データとプログラムデータとすることで、第３者が暗号化されたデータを解読することを困難とするものであり、更に、データの暗号化及び復号化するプログラマブル理論ゲートを集積回路内に設けることで、外部から暗号化・復号化の方法を検出できないように構成するものである。従って、従来技術５においても、従来技術４と同様に、集積回路内に格納されたデータを複製すること自体を防止するためのものとなっている。

【００１５】

しかしながら、これらのように乱数を使用して暗号化キーを決定する方法においては、記憶メディアの対象がＲＯＭなどのような一般的には書き換え不可能とされる記憶媒体に対する技術であるため、上記のような問題を解決するには至っていない。

【００１６】

このように、従来技術による暗号化及び複合化の方法は、当人以外の第３者に対してデータの機密性を保持するためのもの、若しくは、データ自体を複製不可能にするものであるため、情報（映像情報や音声情報など）を複製することを目的とし、更に、この複製において著作権の侵害となる行為を防止するための方法とはなっていない。

【００１７】

従って、本発明は、上記問題に鑑みなされたもので、映像情報や音声情報といった著作権が設定されている情報を複製するにあたり、複製された情報の使用により著作権が侵害される可能性を排除するための情報暗号化装置及びその方法を提供することを目的とする。

【００１８】

【課題を解決するための手段】

係る目的を達成するために、請求項１記載の発明は、他の端末に対して重複することのない固有情報を格納する固有情報格納手段と、固有情報を基にデータを暗号化する暗号化手段とを有することを特徴とする。

【００１９】

また、請求項２記載の発明は、請求項１記載の情報暗号化装置において、固有情報を基に暗号化手段により暗号化されたデータを復号化する復号化手段をさらに有することを特徴とする。

【００２０】

また、請求項３記載の発明によれば、請求項１または２記載の情報暗号化装置において、固有情報格納手段は、格納した固有情報に対し、読み出すことのみ許可することを特徴とする。

【００２１】

また、請求項４記載の発明は、請求項１から３のいずれかに記載の情報暗号化装置において、暗号化手段により暗号化したデータを格納する記憶手段をさらに有することを特徴とする。

【００２２】

また、請求項５記載の発明によれば、請求項１から４のいずれかに記載の情報暗号化装置において、記憶手段は、実際にデータが書き込まれる記憶媒体が交換されないように構成されていることを特徴とする。

【００２３】

また、請求項６記載の発明によれば、請求項１から４のいずれかに記載の情報暗号化装置において、記憶手段は、実際にデータが書き込まれる記憶媒体が交換されるように構成されていることを特徴とする。

【００２４】

また、請求項７記載の発明は、請求項１から５のいずれかに記載の情報暗号化装置において、データを取り込むデータ取込手段をさらに有することを特徴とする。

【００２５】

また、請求項８記載の発明によれば、請求項１から６のいずれかに記載の情報暗号化装置において、固有情報格納手段は、ユーザに到達する以前に固有情報が格納されることを特徴とする。

【００２６】

また、請求項９記載の発明によれば、請求項１から８のいずれかに記載の情報暗号化装置において、固有情報格納手段は、レジスタにより構成されていることを特徴とする。

【００２７】

また、請求項１０記載の発明によれば、請求項１から９のいずれかに記載の情報暗号化装置において、固有情報は、各端末に割り当てられたシリアルナンバーであることを特徴とする。

【００２８】

また、請求項１１記載の発明は、他の端末に対して重複することのない固有情

報を基にデータを暗号化する暗号化工程を有することを特徴とする。

【００２９】

また、請求項１２記載の発明は、請求項１１記載の情報暗号化方法において、固有情報を基に暗号化工程において暗号化されたデータを復号化する復号化工程をさらに有することを特徴とする。

【００３０】

また、請求項１３記載の発明によれば、請求項１１または１２記載の情報暗号化方法において、固有情報は、ユーザにより変更されないように保持されていることを特徴とする。

【００３１】

また、請求項１４記載の発明は、請求項１１から１３のいずれかに記載の情報暗号化方法において、暗号化工程において暗号化したデータを格納する記憶工程をさらに有することを特徴とする。

【００３２】

また、請求項１５記載の発明によれば、請求項１１から１４のいずれかに記載の情報暗号化方法において、記憶工程は、実際にデータが書き込まれる記憶媒体が交換されないように構成されている記憶媒体に暗号化したデータを書き込むことを特徴とする。

【００３３】

また、請求項１６記載の発明によれば、請求項１１から１４のいずれかに記載の情報暗号化方法において、記憶工程は、実際にデータが書き込まれる記憶媒体が交換されるように構成されている記憶媒体に暗号化したデータを書き込むことを特徴とする。

【００３４】

また、請求項１７記載の発明は、請求項１１から１５のいずれかに記載の情報暗号化方法において、暗号化工程の前に、データを取り込むデータ取込工程をさらに有することを特徴とする。

【００３５】

また、請求項１８記載の発明によれば、請求項１１から１７のいずれかに記載

の情報暗号化方法において、固有情報は、レジスタに格納されていることを特徴とする。

【００３６】

また、請求項１９記載の発明によれば、請求項１１から１８のいずれかに記載の情報暗号化方法において、固有情報は、各端末に割り当てられたシリアルナンバーであることを特徴とする。

【００３７】

【発明の実施の形態】

以下、図面を用いて本発明の情報暗号化装置及びその方法を詳細に説明する。

【００３８】

（本発明の特徴）

先ず、本発明の情報暗号化装置及びその方法における特徴を先に述べると、本発明は、パーソナルコンピュータ等の情報処理機器が備える情報記憶媒体に外部情報を複製する方法において、その複製された情報の使用範囲をその複製処理を行った情報処理機器に制限するように構成されている。

【００３９】

従って、本発明の一実施形態を示す図１にあるように、パーソナルコンピュータ等の情報処理機器１は、内部の個別情報格納部４に各情報処理機器１毎に違う（ユニークである）個別情報を保持し、この個別情報を暗号化キーとして外部情報源７から入力された情報を暗号化して内部記憶媒体５に格納することにより、暗号化を行った情報処理機器１のみにその暗号化後の情報の利用を制限するように構成している。

【００４０】

また、内部記憶媒体５に記憶した情報を利用するときは、各情報処理機器１毎の個別情報を予め個別情報格納部４から読み出し、この読み出した個別情報を復号化キーとして利用して復号化する。

【００４１】

以上のように構成することで、作成された内部記憶媒体５上の情報は、これを

作成した情報処理機器１でのみ使用することが可能となる。これは、復号化に必要な復号化キーが暗号化を行った情報処理機器以外では判別できないためである。

【００４２】

（第１の実施形態）

次に、本発明の第１の実施形態を図面を用いて詳細に説明する。

【００４３】

（第１の実施形態の構成）

先ず、第１の実施形態の構成を図１を用いて詳細に説明する。

図１を参照すると、第１の実施形態は、パーソナルコンピュータ等の情報処理機器１と、この情報処理機器１と接続された外部情報源７とにより構成されている。

【００４４】

ここで、外部情報源７としては、ネットワークを介して接続された他の情報処理機器であってもよいし、また、ＡＶ機器等の記憶メディアに記憶された情報を出力する機器であってもよい。これは、本発明が外部情報源７をある特定の機器に限定するものではなく、情報を情報処理機器１に入力するものであれば、本発明の趣旨を逸脱しない限り、適用することが可能なためである。従って、第１の実施形態では、例として外部情報源７がＣＤドライブやＤＶＤドライブ等のＡＶ機器である場合について説明し、外部情報源７がネットワークを介している例の場合を他の実施形態により説明する。

【００４５】

また、情報処理機器１は、各種ソフトウエアを実行する中央演算部２と、ソフトウエアとそのソフトウエアが生成するデータとを一時的に格納しておくためのプログラム格納部３と、情報処理機器１を個別に識別するための個別情報を保持している個別情報格納部４と、不揮発性の記憶媒体である内部記憶装置５と、これら各構成要素を電気的に接続され、制御命令や情報等の伝達を担う制御部６とにより構成されている。

【００４６】

ここで、個別情報は、所定のビット数により構成されるものであり、従来における暗号化／復号化キーと同様の形態で構成することが可能である。

【００４７】

内部記憶媒体５は、所謂ハードディスクドライブ等の大容量記憶媒体で構成することが一般的であるが、本発明ではこれに限定されることなく、例えば、内部機器として書き込み可能なＣＤ－ＲドライブやＤＶＤドライブ等といった記憶媒体を交換することが可能な記憶メディアに対しても適用することが可能である。

【００４８】

従って、本発明では、比較的大容量の記憶容量を有する記憶媒体であれば、本発明の趣旨を逸脱しない限り適用することは可能である。ここで、第１の実施形態では、一例として内部記憶媒体５がＨＤＤ等の実際にデータが書き込まれる媒体が交換できるように構成されていない記憶メディアである場合について説明し、他の実施形態で、例として内部記憶媒体５がＣＤ－ＲドライブやＤＶＤドライブといった、実際にデータが記憶される媒体が交換できるように構成されている記憶メディアである場合について説明する。

【００４９】

また、第１の実施形態では、内部記憶媒体５としてＨＤＤ等のような記憶媒体を交換できないように構成された記憶メディアを使用しているため、この内部記憶媒体５には、暗号化及び復号化の処理プロセスを記述してあるソフトウエア及び暗号化後の情報が格納されている。

【００５０】

但し、本第１の実施形態では、内部記憶媒体５を１台で構成するように示しているが、この内部記憶媒体６は、１台の記憶媒体における記憶領域にパーティションを切ることにより擬似的に複数の内部記憶媒体を設定した場合や実際に複数の内部記憶媒体を備えている場合等であっても、本発明を実現することが可能であるため、１台以上の内部記憶媒体を図１に示すように１つの内部記憶媒体５として表現する。

【００５１】

更に、上記の処理プロセスを記述してあるソフトウエアは、図１における内部記憶媒体５に格納されることに限定されるものではなく、実行する上で逐次読み出せることが可能であれば、本発明の趣旨を逸脱しない限り、如何なる記憶メディアの形態でも適用することが可能である。

【００５２】

また、固有情報格納部４は、所謂ＲＯＭ等の書き換え不可能な記憶媒体により構成する。この固有情報格納部４には、製品出荷時等の段階で各情報処理機器毎に異なる情報を格納しておく。

【００５３】

中央演算部２は、所謂ＣＰＵ（Central Processor Unit）等を意味し、暗号化及び復号化の処理を上記の処理プロセスを記述してあるソフトウエアに従い実行する。

【００５４】

プログラム格納部３は、所謂ＲＡＭ（Random Access Memory）等の高速な記憶メディアにより構成され、一時的にソフトウエア及び各種データを格納しておく。

【００５５】

制御部６は、上記の内部記憶媒体５と固有情報格納部４と中央演算部２とプログラム格納部３とに対してそれぞれに合わせたインタフェースを持ってそれぞれと接続し、各構成要素間での情報の伝達を担う。更に制御部６は、外部情報源７へのアクセスも担う。

【００５６】

外部情報源７は、ＣＤやＤＶＤ等による配布情報の入力源であり、一般的にＡＶ機器として称されるものである。

【００５７】

また、中央演算部２と制御部６とはＣＰＵバス９で接続され、中央演算部２の要求に従い制御部６より各部へアクセス命令が発行される。また、プログラム格納部３と制御部６とはメモリバス１０で接続され、制御部６から発行されたコマンドがプログラム格納部３へ入力されてプログラム格納部３に格納されているデ

ータの読み込み／書き込みが制御される。また、固有情報格納部４と制御部６とはシステムバス１１で接続され、制御部６により必要に応じて固有情報格納部４に格納されている固有情報の読み出し制御が行われる。また、内部記憶媒体５と制御部６とはＨＤバス１２で接続され、制御部６により内部記憶媒体５への読み込み／書き込み制御が行われる。更に外部情報源７と制御部６とは外部メディアバス８で接続され、制御部６により外部情報源７への読み込み／書き込み制御が行われる。

【００５８】

（第１の実施形態の動作）

次に、図１から図３を用いて第１の実施形態の動作を詳細に説明する。

本動作における動作は、外部情報源７より入力された情報を暗号化する動作と、この暗号化した情報を復号化する動作との２つに大きく分類することができる。

【００５９】

ここで図２は、本発明において、暗号化処理を行うソフトウエアの流れを示すフローチャートである。

【００６０】

図２に示すように、暗号化処理が開始されると、本発明による情報暗号化装置及びその方法は、先ず固有情報格納部４から格納されている固有情報を読み込む（ステップＳ０１）。この読み込まれた固有情報は、中央演算部２内に暗号化キーとして保持される。

【００６１】

次に、外部情報源７から暗号化の対象となる情報を読み込み、プログラム格納部３に一時保持する（ステップＳ０２）。この処理は、中央演算部２からの命令に従い、制御部６の制御により実行される。

【００６２】

続いて、中央演算部２がプログラム格納部３に格納されている情報を読み込み、この読み込んだ固有情報を暗号化キーとして所定の情報量毎に暗号化し、このように暗号化された情報を逐次プログラム格納部３に書き込む（ステップＳ０３

）。ここで暗号化の方法については、多くの技術が開示されているが、本発明では、この暗号化方法を特に限定せず、暗号化キーとして本発明による固有情報を適用することが可能である暗号化方法であれば、本発明の趣旨を逸脱しない限り、如何なる方法でも適用することが可能である。

【００６３】

その後、プログラム格納部３に格納された暗号化後の情報を内部記憶媒体５に書き込む（ステップＳ０４）。この処理は、中央演算部２が暗号化後の情報をプログラム格納部３から読み出して内部記憶媒体５に書き込むという処理を実行する方法と、中央演算部２が制御部６に命令を与え、この与えられた命令に基づいて制御部６がプログラム格納部３から内部記憶媒体５へ情報の転送を行う方法とが考えられる。

【００６４】

また、図３は、上記のように暗号化した情報に対して複合化処理を施すソフトウエアの流れを示すフローチャートである。

【００６５】

図３に示すように、復号化処理が開始されると、先ず暗号化処理と同様に、固有情報格納部４から固有情報が読み込まれ、中央演算部２内部に復号化キーとして保持される（ステップＳ１１）。

【００６６】

続いて、中央演算部２がプログラム格納部３から暗号化データを読み込み、プログラム格納部３に格納する（ステップＳ１２）。

【００６７】

次に、中央演算部２がプログラム格納部３からステップＳ１２で格納した暗号化後の情報を読み込み、この暗号化後の情報をステップＳ１１で保持した復号化キーを用いて所定の情報量毎に逐次復号化を行い、復号化後の情報をプログラム格納部３に書き込む（ステップＳ１３）。ここで、本発明における複合化の方法としては、上記の暗号化方法に対応した方法を用いることで、実現することが可能である。このため、暗号化に用いた方法が、シャフリングによる暗号化方法であればデシャフリングを、また、スクランブルによる暗号化方法であればデスク

ランブルを複合化の方法として用いる。これは、暗号化／復号化を同一のソフトウエアにより実行する場合、そのソフトウエア内で統一するという発想により実現されるものである。

【００６８】

上記のように、復号化処理に使用する復号化キーは、暗号化処理に使用した暗号化キーと同一のものでなければならないため、復号化が可能な情報処理機器は必然的に暗号化を実行した情報処理機器に限定される。

【００６９】

このように、復号化後に得られた情報は、それが画像データであれば画像表示が、音声データであれば音声再生が、文書データであれば文書表示がされることになるが、これらに対する処理のフローに関しては、本発明では特に限定するものではない。

【００７０】

また、暗号化されて内部記憶媒体５に格納された情報は、他の記憶媒体、例えばフロッピーディスクやＣＤ－Ｒ等に複製することも可能であるが、このように複製した情報に対しても、利用可能なように制限されている情報処理機器は、その情報を生成した情報処理機器に限定されていることは当然である。

【００７１】

（第２の実施形態）

次に、本発明の第２の実施形態について図面を用いて詳細に説明する。

図４は、第２の実施形態による情報暗号化装置及びその方法の構成を示すブロック図である。

【００７２】

図４を参照すると、第２の実施形態では、第１の実施形態と同様の箇所として、情報処理機器１における中央演算部２、プログラム格納部３及び内部記憶媒体５があり、第１の実施形態との相違点として、第１の実施形態における固有情報格納部４が制御部６における書き込み／読み出し可能なデータ保持機能（一般的にレジスタと呼ばれるもの）を使用して構成されている点がある。

【００７３】

従って、第２の実施形態における制御部６は、その内部に個別情報レジスタ１３を有して構成されている。しかしながら、本発明では、格納している個別情報の書き換えが不可能でなければならないため、上記の個別情報レジスタ１３は、ワンタイムＲＯＭ等のような１度書き込んだ情報を書き換えることが不可能なもので実現する。

【００７４】

このような書き換え不可能な記憶媒体を個別情報レジスタ１３に使用し、本発明の情報処理機器１を製造する過程において１台１台異なるデータ（所謂シリアルナンバー）を上記の個別情報レジスタ１３に格納することにより、書き換え不可能で、更に個々の情報処理機器においてユニークな個別情報を情報処理機器１内部に作成することが可能である。

【００７５】

また、外部情報源７としては、第１の実施形態での説明と同様である。

【００７６】

従って、第１の実施形態による個別情報格部４では、この個別情報格納部４がＲＯＭ等で使用されることが一般的であるため、これを情報処理機器１から取り外して複製し、交換することが容易であったが、第２の実施形態では、以上のように構成することで、第１の実施形態と比較して、この制御部６を交換することが困難であり、更に個別情報を読み出して複製するということが不可能となるように構成することが可能となる。

【００７７】

また、第２の実施形態では、第１の実施形態における動作と同様の流れにより実現することが可能である。

【００７８】

（第３の実施形態）

また、本発明の第３の実施形態について図面を用いて詳細に説明する。

図５は、第３の実施形態による情報暗号化装置及びその方法の構成を示すブロック図である。

【００７９】

図５を参照すると、第３の実施形態では、第１の実施形態と同様の箇所として、情報処理機器１におけるプログラム格納部３、内部記憶媒体５及び制御部６があり、第１の実施形態との相違点として、第２の実施形態における固有情報レジスタ１３が中央演算部２内に設けられている点がある。

【００８０】

近年、中央演算部６（ＣＰＵ）内部にシリアルナンバーを格納するように構成されているため、第３の実施形態では、固有情報としてこのシリアルナンバーを使用するように構成する。

【００８１】

この構成により、第１の実施形態及び第２の実施形態で示したように、固有情報を格納する手段として、特別な記憶媒体を設ける必要がなくなり、装置規模の縮小を達成することが可能となる。

【００８２】

また、外部情報源７としては、第１の実施形態での説明と同様である。

【００８３】

また、第３の実施形態では、第１の実施形態及び第２の実施形態における動作と同様の流れにより実現することが可能である。

【００８４】

（第４の実施形態）

次に、本発明の第４の実施形態について図面を用いて詳細に説明する。

第４の実施形態では、第１の実施形態で触れたように、情報処理機器１がネットワークと接続されており、外部情報源がこのネットワーク上の端末である場合についての一実施形態である。

【００８５】

図６を参照すると、本発明の第４の実施形態では、第１の実施形態と同様の箇所として、情報処理機器１における中央演算部２、プログラム格納部３、個別情報記憶部４及び内部記憶媒体５があり、第１の実施形態との相違点として、制御部１４が第１の実施形態における制御部６に対して更にネットワークインタフェースとしての機能を有するように構成されている点がある。

【００８６】

従って、制御部１４とネットワーク１５とはネットワーク回線１６を介して接続されている。

【００８７】

ここで、制御部１４を介して接続されているネットワーク１５には、多数のネットワーク端末が接続されていると考えられるが、本発明では、これらの端末を限定するものではなく、情報源として機能するものであれば、本発明の趣旨を逸脱しない限り全て適用することが可能である。

【００８８】

上記のように構成することで、第４の実施形態では、ネットワークを介して接続された端末を外部情報源として機能させることが可能である。

【００８９】

また、第４の実施形態では、第１の実施形態から第３の実施形態における動作と同様の流れにより実現することが可能である。

【００９０】

（第５の実施形態）

次に、本発明の第５の実施形態について図面を用いて詳細に説明する。

第５の実施形態では、第１の実施形態で触れたように、内部記憶媒体に、実際にデータが記憶される媒体が交換できるように構成されている記憶メディアを適用している場合についての一実施形態である。

【００９１】

図７を参照すると、本発明の第５の実施形態では、第１の実施形態と同様の箇所として、情報処理機器１における中央演算部２、プログラム格納部３及び個別情報記憶部４があり、第１の実施形態との相違点として、内部記憶媒体５の替わりに、実際にデータが記憶される媒体が交換できるように構成されている内部記憶媒体１７が備えられている点である。

【００９２】

従って、制御部６と内部記憶媒体１７とは、内部記憶メディアバス１８を介して接続されている。

【００９３】

また、第５の実施形態では、第１の実施形態から第４の実施形態における動作と同様の流れにより実現することが可能である。

【００９４】

（上記各実施形態の重複）

更に、上記した各実施形態は、各実施形態の構成をそれぞれ組み合わせて実施することも可能である。

【００９５】

【発明の効果】

以上説明したように、本発明の情報暗号化装置及びその方法によれば、映像情報や音声情報等といった著作権の設定がされた情報を複製する場合に、複製された情報の使用範囲をその複製を実行した情報処理機器に制限することにより、複製された情報により著作権が侵害される可能性を除去することが可能となる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態の構成を示すブロック図である。

【図２】

本発明における暗号化処理の動作の流れを示すフローチャートである。

【図３】

本発明における複合化処理の動作の流れを示すフローチャートである。

【図４】

本発明の第２の実施形態の構成を示すブロック図である。

【図５】

本発明の第３の実施形態の構成を示すブロック図である。

【図６】

本発明の第４の実施形態の構成を示すブロック図である。

【図７】

本発明の第５の実施形態の構成を示すブロック図である。

【符号の説明】

１　情報処理機器

２　中央演算部

３　プログラム格納部

４　固有情報格納部

５、１７　内部記憶媒体

６、１４　制御部

７　外部情報源

８　外部メディアバス

９　ＣＰＵバス

１０　メモリバス

１１　システムバス

１２　ＨＤバス

１３　固有情報レジスタ

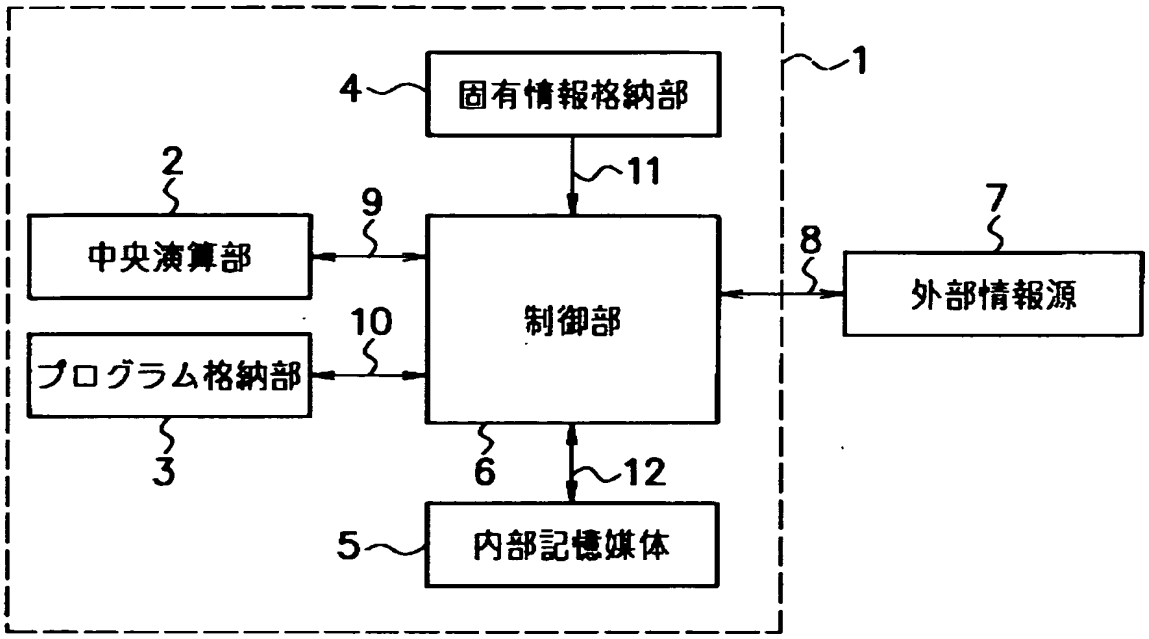
１５　ネットワーク網

１６　ネットワーク回線

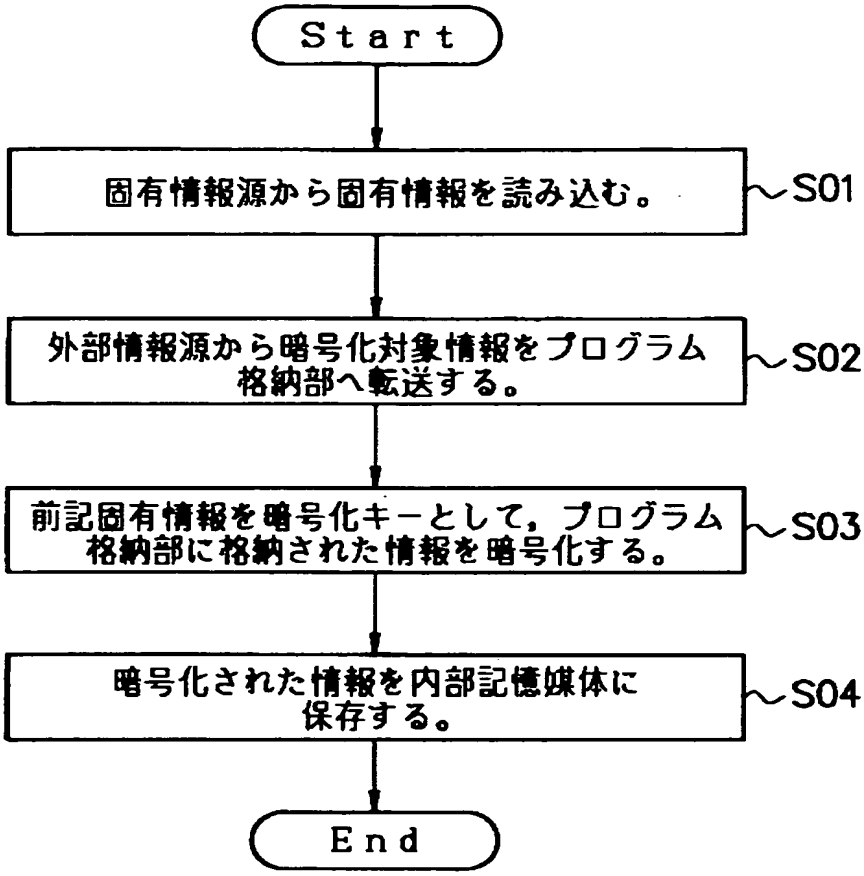
１８　内部記憶メディアバス

【書類名】　　図面

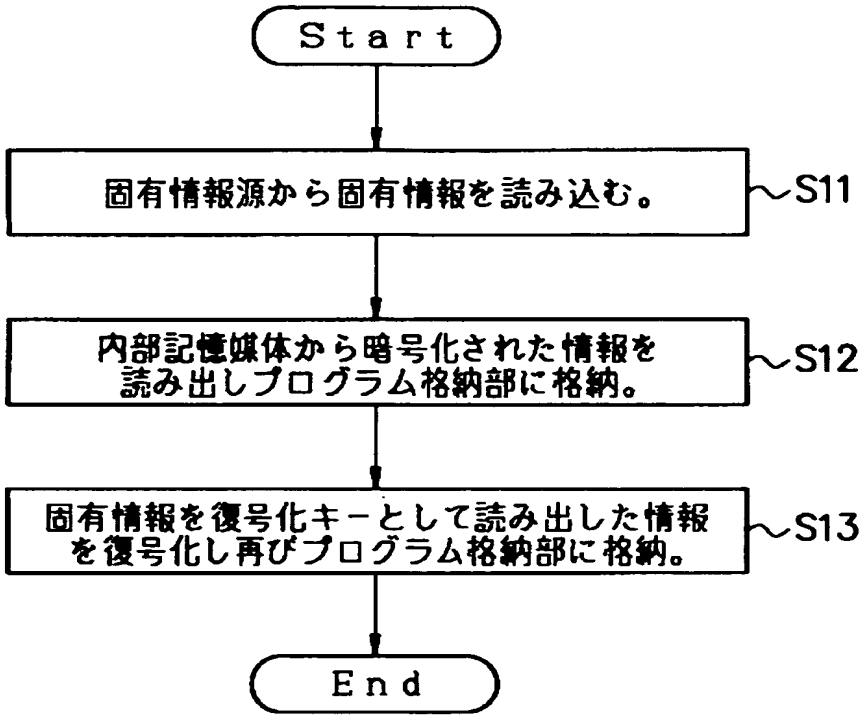
【図１】



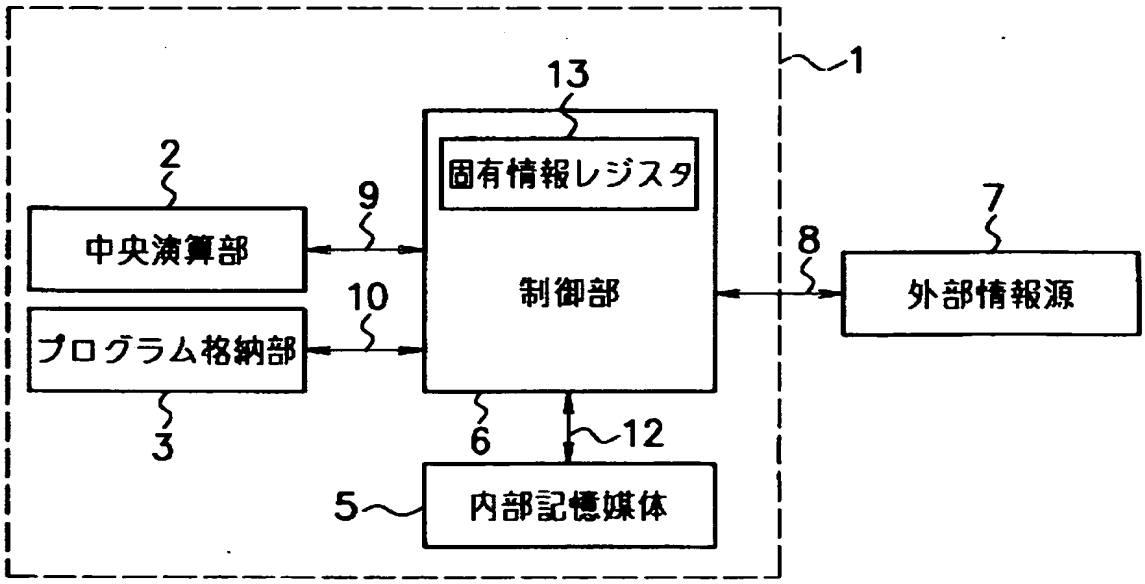
【図２】


Start
固有情報源から固有情報を読み込む。
S01
外部情報源から暗号化対象情報をプログラム格納部へ転送する。
S02
前記固有情報を暗号化キーとして，プログラム格納部に格納された情報を暗号化する。
S03
暗号化された情報を内部記憶媒体に保存する。
S04
End

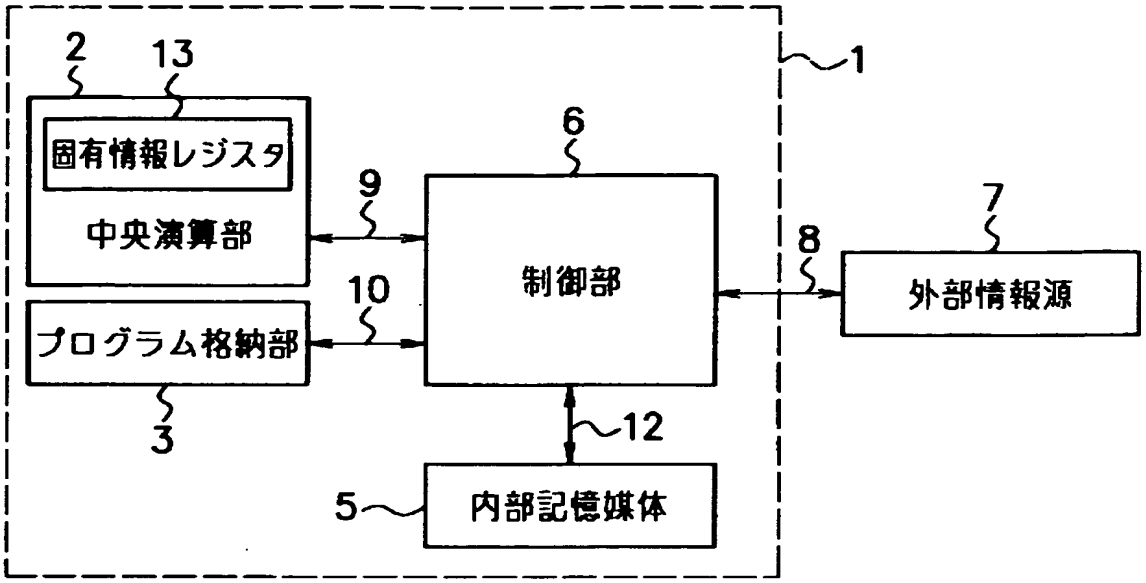
【図３】


Start
固有情報源から固有情報を読み込む。
S11
内部記憶媒体から暗号化された情報を
読み出しプログラム格納部に格納。
S12
固有情報を復号化キーとして読み出した情報
を復号化し再びプログラム格納部に格納。
S13
End

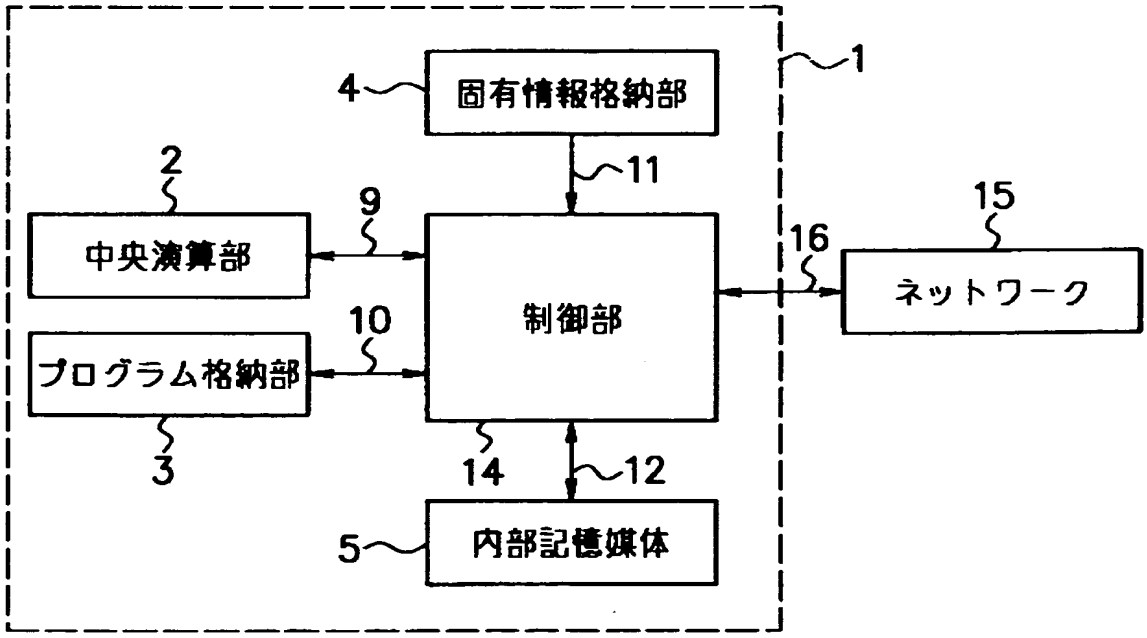
【図４】


1
13
固有情報レジスタ
2
9
中央演算部
7
8
外部情報源
制御部
10
プログラム格納部
3
6
12
5
内部記憶媒体

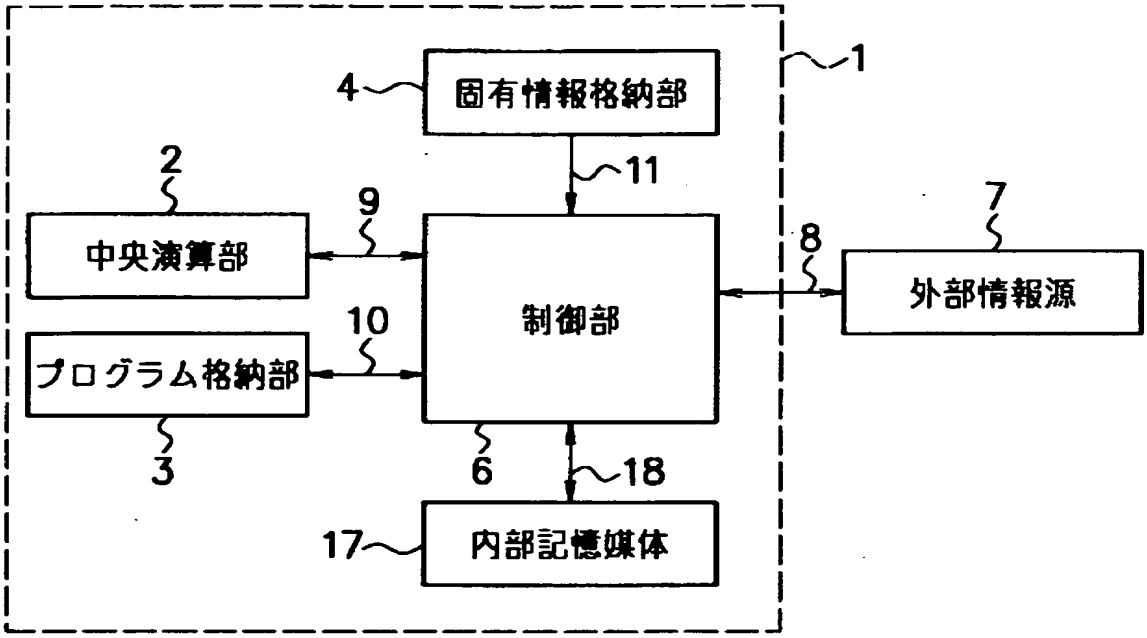
【図５】


2
13
1
固有情報レジスタ
中央演算部
9
6
制御部
8
7
外部情報源
10
プログラム格納部
3
12
5
内部記憶媒体

【図６】


1
4
固有情報格納部
11
2
9
15
中央演算部
16
制御部
ネットワーク
10
プログラム格納部
3
14
12
5
内部記憶媒体

【図７】


1
4
固有情報格納部
11
2
9
中央演算部
7
8
外部情報源
10
制御部
プログラム格納部
3
6
18
17
内部記憶媒体

【書類名】　　要約書

【要約】

【課題】　著作権が設定されている情報を複製するにあたり、複製された情報の使用により著作権が侵害される可能性を排除するための情報暗号化装置及びその方法を提供する。

【解決手段】　情報処理機器１を、各種ソフトウエアを実行する中央演算部２と、ソフトウエアとそのソフトウエアが生成するデータとを一時的に格納しておくためのプログラム格納部３と、情報処理機器１を個別に識別するための個別情報を保持している個別情報格納部４と、不揮発性の記憶媒体である内部記憶装置５と、これら各構成要素を電気的に接続され、制御命令や情報等の伝達を担う制御部６とにより構成し、固有情報格納部４を、所謂ＲＯＭ等の書き換え不可能な記憶媒体により構成し、製品出荷時等の段階で各情報処理機器毎に異なる情報を格納しておく。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００１９０５４１〕

１．変更年月日　１９９０年　８月１０日
［変更理由］　新規登録
住　所　新潟県柏崎市大字安田７５４６番地
氏　名　新潟日本電気株式会社